

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-264655

(43)Date of publication of application : 06.10.1998

(51)Int.Cl.

B60J 5/00

(21)Application number : 09-094683

(71)Applicant : TOYODA GOSEI CO LTD

(22)Date of filing : 27.03.1997

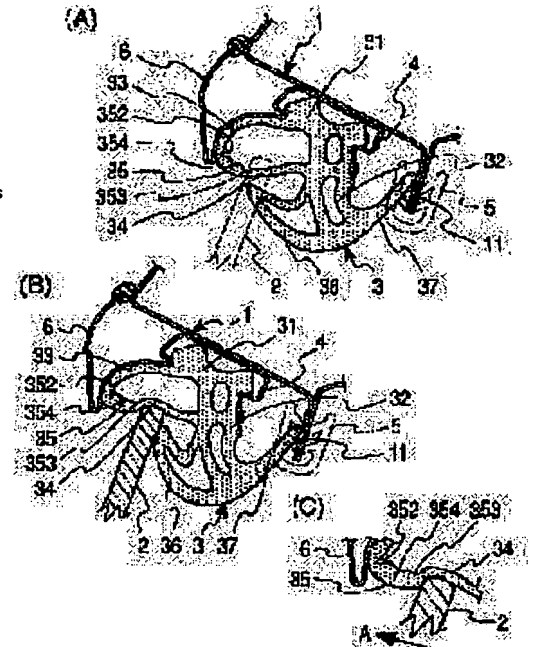
(72)Inventor : OKADA MASAYASU

## (54) WEATHER STRIP FOR AUTOMOBILE

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To achieve favorable sealability around a door glass, and prevent the outward suction of the door glass in high speed run of an automobile.

**SOLUTION:** A curvature corner part 35 of a hollow weather strip 3 installed on a door aperture edge 1 of a car body is formed thicker than a seal wall 34, notches 352, 353 are respectively formed on an inner surface at both ends connected to a side wall 33 of the corner part 35 and the seal wall 34 to let the seal wall 34 deformed when it is pushed up by a door glass 2, and a notch 354 of a smaller groove width than the notches 352, 353 is formed at a middle position between them, so outward suction of the door glass 2 is prevented by the corner part 35 having a cross sectional surface in a gentle V-form by closing the notch 354 caught between a mould 6 provided on the door aperture edge 1 and the door glass 2.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 特 許 公 報 (B 1)

(11)特許番号

特許第3002184号

(P3002184)

(45)発行日 平成12年1月24日(2000.1.24)

(24)登録日 平成11年11月12日(1999.11.12)

(51)Int.Cl.<sup>7</sup>

識別記号

F I

H 0 4 L 9/14  
9/32

H 0 4 L 9/00

6 4 1  
6 7 3 B  
6 7 5 A

請求項の数6(全 15 頁)

(21)出願番号 特願平10-264655

(22)出願日 平成10年9月18日(1998.9.18)

審査請求日 平成10年9月18日(1998.9.18)

(73)特許権者 000004226

日本電信電話株式会社  
東京都千代田区大手町二丁目3番1号

(72)発明者 庵 祥子

東京都新宿区西新宿三丁目19番2号 日  
本電信電話株式会社内

(72)発明者 玉井 誠

東京都新宿区西新宿三丁目19番2号 日  
本電信電話株式会社内

(72)発明者 三宅 延久

東京都新宿区西新宿三丁目19番2号 日  
本電信電話株式会社内

(74)代理人 100083806

弁理士 三好 秀和 (外1名)

審査官 青木 重徳

最終頁に続く

(54)【発明の名称】 コンテンツ利用装置とコンテンツ利用プログラムを記録した記録媒体

1

(57)【特許請求の範囲】

【請求項1】 暗号化されたコンテンツと、当該暗号化されたコンテンツを復号する第1の復号鍵とを取得し、所定の端末識別情報および提供される利用者認証情報で前記復号鍵をそれぞれ暗号化して得られる第2、第3の復号鍵を記憶する記憶手段と、前記暗号化されたコンテンツを復号するに際し、この暗号化されたコンテンツを復号する利用端末の端末識別情報により前記記憶手段に記憶される第2の復号鍵の復号が可能かどうかを判定する判定手段と、この判定手段で復号可能であると判定されたときには、この端末識別情報により前記暗号化された第2の復号鍵を復号化して第1の復号鍵を得、不可能であると判定されたときには、前記利用者認証情報により前記暗号化された第3の復号鍵を復号化して第1の復号鍵を得る復号

2

手段とを有することを特徴とするコンテンツ利用装置。

【請求項2】 暗号化されたコンテンツと、当該暗号化されたコンテンツを復号する第1の復号鍵とを取得し、所定の端末識別情報および提供される利用者認証情報で前記復号鍵をそれぞれ暗号化して得られる第2、第3の復号鍵と、任意の所定値を前記端末識別情報で暗号化して得られる暗号値とを記憶する記憶手段と、前記暗号化されたコンテンツを復号するに際し、この暗号化されたコンテンツを復号する利用端末の端末識別情報により前記任意の所定値を暗号化し、この値と前記記憶手段に記憶される暗号値とを比較する判定手段と、この判定手段で一致したと判定されたときには、この端末識別情報により前記暗号化された第2の復号鍵を復号化して第1の復号鍵を得、一致しないと判定されたときには、前記利用者認証情報により前記暗号化された第3

の復号鍵を復号化して第1の復号鍵を得る復号手段とを有することを特徴とするコンテンツ利用装置。

【請求項3】 前記利用者認証情報が、利用者IDと利用者パスワードの組み合わせであることを特徴とする請求項1または2記載のコンテンツ利用装置。

【請求項4】 前記端末識別情報が、各端末毎に端末に付与されるIDであることを特徴とする請求項1または2記載のコンテンツ利用装置。

【請求項5】 暗号化されたコンテンツと、当該暗号化されたコンテンツを復号する第1の復号鍵とを取得し、所定の端末識別情報および提供される利用者認証情報で前記復号鍵をそれぞれ暗号化して第2、第3の復号鍵を用意し、

前記暗号化されたコンテンツを復号するに際し、この暗号化されたコンテンツを復号する利用端末の端末識別情報により前記暗号化された第2の復号鍵の復号が可能かどうかを判定し、

復号可能であるときには、この端末識別情報により前記暗号化された第2の復号鍵を復号化して第1の復号鍵を得、

不可能であるときには、前記利用者認証情報により前記暗号化された第3の復号鍵を復号化して第1の復号鍵を得ることを特徴とするコンテンツ利用プログラムを記録した記録媒体。

【請求項6】 暗号化されたコンテンツと、当該暗号化されたコンテンツを復号する第1の復号鍵とを取得し、所定の端末識別情報および提供される利用者認証情報で前記復号鍵をそれぞれ暗号化して第2、第3の復号鍵と、任意の所定値を前記端末識別情報で暗号化して得られる暗号値とを用意し、

前記暗号化されたコンテンツを復号するに際し、この暗号化されたコンテンツを復号する利用端末の端末識別情報により前記任意の所定値を暗号化し、この値と前記暗号値とを比較し、

一致したときには、この端末識別情報により前記暗号化された第2の復号鍵を復号化して第1の復号鍵を得、

一致しないときには、前記利用者認証情報により前記暗号化された第3の復号鍵を復号化して第1の復号鍵を得ることを特徴とするコンテンツ利用プログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、暗号化されたデジタルコンテンツを流通・配布するのに適したコンテンツ利用装置とコンテンツ利用プログラムを記録した記録媒体に関するものである。

【0002】

【従来の技術】近年、プログラムを含むあらゆる情報がインターネットやCD-ROMなどのメディアを介して、いわゆるコンテンツとして流通・配布されるに至っ

ている。このようなコンテンツはデジタル化され、デジタルコンテンツとしてさらに暗号化が施されて流通・配布される場合がある。

【0003】このように暗号化したデジタルコンテンツの流通・配布に際して、暗号化したデジタルコンテンツの復号鍵を端末識別装置を用いて取り出した「端末固有番号」のみを鍵にして暗号化することが想定される。この場合には、不正使用の防止を実現し得るが、正規の利用者でもデジタルコンテンツを他の端末に複製することが不可能であるという問題がある。

【0004】一方、暗号化したデジタルコンテンツの復号鍵を「利用者IDと利用者パスワードの組み合わせ」のみを鍵にして暗号化することが想定される。この場合には、正規の利用者以外でも他端末に複製することが可能であるということ、デジタルコンテンツを利用するときには必ず利用者に「利用者IDと利用者パスワードの組み合わせ」を入力させなければならないという問題がある。

【0005】

【発明が解決しようとする課題】すなわち、暗号化されたデジタルコンテンツの流通・配布にあつては、下記に示すような解決すべき課題があった。

【0006】1. 正規の利用者が「利用者IDと利用者パスワードの組み合わせ」を入力することによって他端末へデジタルコンテンツを複製することを可能にし、同時に利用者以外には他端末へのデジタルコンテンツの複製を不可能にすることによって不正使用を防止すること。

【0007】2. 暗号化されたデジタルコンテンツの復号鍵を一度でも「利用者IDと利用者パスワードの組み合わせ」によって復号した場合は、それ以後復号されたときと同じ端末に格納されている限りは再び「利用者IDと利用者パスワードの組み合わせ」を入力する必要をなくすること。

【0008】本発明は、上記課題に鑑みてなされたもので、これら課題を解決することのできるコンテンツ利用装置とコンテンツ利用プログラムを記録した記録媒体を提供することを目的とする。

【0009】

【課題を解決するための手段】前述した目的を達成するために、本発明のうちで請求項1記載の発明は、暗号化されたコンテンツと、当該暗号化されたコンテンツを復号する第1の復号鍵とを取得し、所定の端末識別情報および提供される利用者認証情報で前記復号鍵をそれぞれ暗号化して得られる第2、第3の復号鍵を記憶する記憶手段と、前記暗号化されたコンテンツを復号するに際し、この暗号化されたコンテンツを復号する利用端末の端末識別情報により前記記憶手段に記憶される第2の復号鍵の復号が可能かどうかを判定する判定手段と、この判定手段で復号可能であると判定されたときには、この端末識別情報により前記暗号化された第2の復号鍵を復

号化して第1の復号鍵を得、不可能であると判定されたときには、前記利用者認証情報により前記暗号化された第3の復号鍵を復号化して第1の復号鍵を得る復号手段とを有することを要旨とする。

【0010】請求項1記載の本発明では、暗号化されたコンテンツの第1の復号鍵を、例えば端末識別装置を用いて取り出した利用端末の端末識別情報と、例えば利用者IDと利用者パスワードの組み合わせによる利用者認証情報のそれぞれを鍵として暗号化し、第2、第3の復号鍵を得、記憶手段に記憶する。

【0011】暗号化されたコンテンツを利用する場合は、端末識別情報が利用者認証情報のどちらかを鍵として暗号化されたコンテンツの第1の復号鍵を記憶手段に記憶される第2あるいは第3の復号鍵で復号し、コンテンツの復号を可能にする。

【0012】また、請求項2記載の発明は、暗号化されたコンテンツと、暗号化されたコンテンツと、当該暗号化されたコンテンツを復号する第1の復号鍵とを取得し、所定の端末識別情報および提供される利用者認証情報で前記復号鍵をそれぞれ暗号化して得られる第2、第3の復号鍵と、任意の所定値を前記端末識別情報で暗号化して得られる暗号値とを記憶する記憶手段と、前記暗号化されたコンテンツを復号するに際し、この暗号化されたコンテンツを復号する利用端末の端末識別情報により前記任意の所定値を暗号化し、この値と前記記憶手段に記憶される暗号値とを比較する判定手段と、この判定手段で一致したと判定されたときには、この端末識別情報により前記暗号化された第2の復号鍵を復号化して第1の復号鍵を得、一致しないと判定されたときには、前記利用者認証情報により前記暗号化された第3の復号鍵を復号化して第1の復号鍵を得る復号手段とを有することを要旨とする。

【0013】請求項2記載の本発明では、暗号化されたコンテンツの第1の復号鍵を、端末識別装置を用いて取り出した所定の端末識別情報（端末識別番号・端末固有番号）と利用者認証情報、例えば利用者IDと利用者パスワード、さらにはクレジットカード番号とその暗証番号、銀行口座番号とその暗証番号のそれぞれを適宜単独にあるいは組み合わせて鍵として暗号化する。また、暗号化されたコンテンツを利用する場合は、端末識別情報か利用者認証情報のどちらかを鍵として暗号化されたコンテンツの第1の復号鍵を復号し、コンテンツの復号を可能にする。

【0014】正規の利用者でも他端末へ複製できないという問題は、暗号化されたコンテンツの複製を可能とし、正規の利用者が複製後初めて復号するときに利用者認証情報を入力して正規の利用者であると認証された場合のみ第1の復号鍵を復号することによって解決する。これにより、正規の利用者以外の他端末への複製を防止することができる。

【0015】この際、入力された利用者認証情報が正しいかどうかの判定を行う。正しくない場合は、正しく第1の復号鍵を復号できない旨を伝えるエラー処理を行う。入力された利用者認証情報が正しい場合には、正しく第1の復号鍵が復号され、暗号化されたコンテンツを復号する。暗号化されたコンテンツが復号できた場合は、新たに格納された端末の端末識別番号で暗号化されたコンテンツの第1の復号鍵を再度暗号化して、以前の端末識別番号で暗号化されたコンテンツの復号鍵に上書きしておく。

【0016】また、利用者が一度でも利用者認証情報で認証したコンテンツに対してはそれ以後、端末固有番号を利用して第1の復号鍵を復号することによって、コンテンツを利用する度に利用者認証情報を入力しなければならないという問題を解決する。

【0017】これにより、他端末への複製に対しては、複製した暗号化されたコンテンツに対し、正規の利用者が利用者認証情報を入力することによって第1の復号鍵を復号することによって可能とし、同時に正規の利用者以外による他端末への複製を防止する。また、暗号化されたコンテンツの第1の復号鍵を一度でも利用者認証情報で復号した端末では、それ以後、端末固有番号を利用して第1の復号鍵の復号をするため利用者認証情報を入力する必要がなくなる。

【0018】

【0019】

【0020】

【0021】

【0022】

【0023】また、請求項3記載の発明は、前記請求項1または2記載の利用者認証情報が、利用者IDと利用者パスワードの組み合わせであることを要旨とする。

【0024】また、請求項4記載の発明は、前記請求項1または2記載の端末識別情報が、各端末毎に端末に付与されるIDであることを要旨とする。

【0025】また、請求項5記載の発明は、記録媒体に、暗号化されたコンテンツと、当該暗号化されたコンテンツを復号する第1の復号鍵とを取得し、所定の端末識別情報および提供される利用者認証情報で前記復号鍵をそれぞれ暗号化して第2、第3の復号鍵を用意し、前記暗号化されたコンテンツを復号するに際し、この暗号化されたコンテンツを復号する利用端末の端末識別情報により前記暗号化された第2の復号鍵の復号が可能かどうかを判定し、復号可能であるときには、この端末識別情報により前記暗号化された第2の復号鍵を復号化して第1の復号鍵を得、不可能であるときには、前記利用者認証情報により前記暗号化された第3の復号鍵を復号化して第1の復号鍵を得ることを特徴とするコンテンツ利用プログラムを記録したことを要旨とする。

【0026】請求項5記載の本発明では、コンテンツ利

用プログラムを記録媒体として記録しているため、該記録媒体を利用して、そのコンテンツ利用プログラムの流通性を高めることができる。

【0027】また、請求項6記載の発明は、記録媒体に、暗号化されたコンテンツと、当該暗号化されたコンテンツを復号する第1の復号鍵とを取得し、所定の端末識別情報および提供される利用者認証情報で前記復号鍵をそれぞれ暗号化して第2、第3の復号鍵と、任意の所定値を前記端末識別情報で暗号化して得られる暗号値とを用意し、前記暗号化されたコンテンツを復号するに際し、この暗号化されたコンテンツを復号する利用端末の端末識別情報により前記任意の所定値を暗号化し、この値と前記暗号値とを比較し、一致したときには、この端末識別情報により前記暗号化された第2の復号鍵を復号化して第1の復号鍵を得、一致しないときには、前記利用者認証情報により前記暗号化された第3の復号鍵を復号化して第1の復号鍵を得ることを特徴とするコンテンツ利用プログラムを記録したことを要旨とする。

【0028】請求項6記載の本発明では、コンテンツ利用プログラムを記録媒体として記録しているため、該記録媒体を利用して、そのコンテンツ利用プログラムの流通性を高めることができる。

【0029】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。

【0030】図1は本発明の一実施例の形態に係るコンテンツ利用装置を含むシステムの構成を示すブロック図である。

【0031】図1において、1は正規利用者が使用する利用者端末であり、この利用者端末1はコンピュータネットワーク3と適宜接続することが可能であるように構成されている。また、このコンピュータネットワーク3には商店端末5が常時、接続され、さらにこのコンピュータネットワーク3には正規利用者以外の利用者端末7も適宜、接続されるものとする。

【0032】また、本実施形態では、上記利用者端末1には、利用者認証情報取得部11、コンテンツ取得部13、端末識別番号取得部15、暗号化部17、記憶部19、判定部21、復号化部23およびコンテンツ利用部25が構成され、カードリーダ31が内蔵され、あるいは着脱自在に接続されているものとする。

【0033】なお、コンテンツ取得部13には暗号化コンテンツ取得部13aと復号鍵取得部13bが構成され、暗号化部17には復号鍵暗号化部17aと所定値暗号化部17bが構成され、復号化部23には暗号化復号鍵復号化部23aとコンテンツ復号化部23bが構成される。

【0034】また、記憶部19には、「暗号化した復号鍵」、「暗号化されたコンテンツ」、「利用者認証情報」、「利用者認証情報暗号化値」、「端末識別番号」

および「端末識別番号暗号化値」を記憶するためのファイルが適宜設けられる。なお、通常は「利用者認証情報」と「端末識別番号」、あるいは「利用者認証情報暗号化値」と「端末識別番号暗号化値」のファイルが適宜設けられる。

【0035】また、これら利用者認証情報取得部11、コンテンツ取得部13、端末識別番号取得部15、暗号化部17、記憶部19、判定部21、復号化部23およびコンテンツ利用部25は、通常、利用者端末1内に予め組み込まれて提供されるが、コンテンツを利用するに際して、コンテンツの流通・配布事業者から通信（無線、有線）または記録媒体を介して提供されるプログラムにより予め構築されるものであっても良い。

【0036】以下、図1を参照して、暗号化されたデジタルコンテンツ利用装置を含むシステムの一実施形態を詳細に説明する。

【0037】まず、端末識別番号取得部15について説明する。

【0038】利用者端末1の記憶部19に、自端末を識別するための端末識別情報としての「端末識別番号」を保持する場合と、そうでない場合がある。「端末識別番号」を保持する場合には、端末識別番号取得部15は、記憶部19のファイル中の「端末識別番号」を取得する。一方、保持しない場合には、端末識別番号取得部15は、OS製品番号または起動ディスクパーティションのシリアルIDまたは起動ディスクパーティションのボリューム名または起動ディスクパーティション容量またはこれらの情報を組み合わせた情報などを「端末識別番号」の代替として取得する。

【0039】次に、判定部21における処理について説明する。ここでは利用者認証情報取得部11において、利用者認証情報、例えば利用者IDと利用者パスワード、より具体的にはクレジットカード番号と銀行口座番号とそれぞれの暗証番号を単独にまたは任意の組み合わせが取得されるものとする。

【0040】a) 利用者認証情報、例えば利用者IDと利用者パスワードをそのまま保存する場合（図2（a）参照）

正規の利用者の、例えば「利用者IDと利用者パスワードの組み合わせ」を予め記憶部19の「利用者認証情報」ファイルに保存しておく。そして利用者認証情報取得部11を介して入力された「利用者IDと利用者パスワードの組み合わせ」と記憶部19に保存してある「利用者IDと利用者パスワードの組み合わせ」とを判定部21において比較し、正しいかどうかを判定し、その判定結果を音声・画面表示として出力する。

【0041】b) 利用者認証情報、例えば利用者IDと利用者パスワードを鍵にして所定値A0を暗号化して保存する場合（図2（b）参照）

暗号化部17の所定値暗号化部17bは、予め、ある任

意に設定される所定値A0を正規の利用者の「利用者IDと利用者パスワードの組み合わせ」を鍵として暗号化すると共に、この暗号化結果を利用者認証情報暗号化値A1として記憶部19に保存しておく。そして利用者認証情報取得部11を介して「利用者IDと利用者パスワードの組み合わせ」が入力されたときには、この「利用者IDと利用者パスワードの組み合わせ」を鍵として、所定値A0を暗号化する。この暗号結果をA2とする。判定部21は、A1とA2を比較し、正しいかどうかを判定し、その判定結果を音声・画面表示として出力する。

【0042】次に、図3乃至図5を参照して、鍵ファイルを暗号化されたデジタルコンテンツのファイルに付加するタイプにおけるデジタルコンテンツ利用方法を具体的に説明する。

【0043】図3において、ステップS11で、利用者は利用者端末1を操作して、商店端末5からコンピュータネットワーク3を介して、暗号化されたデジタルコンテンツをダウンロードする。また、ダウンロードと同時に、あるいは該暗号化されたデジタルコンテンツの暗号化されていない目次もしくは見出し情報を参照して、当該デジタルコンテンツの購入を決定したときに、ステップS13において暗号化されたデジタルコンテンツの復号鍵を購入する。

【0044】そしてステップS15において、購入した暗号化されたデジタルコンテンツの復号鍵を「利用者IDと利用者パスワードの組み合わせ」と、利用者認証情報取得部11を用いて取り出した利用者端末1の「端末識別番号」の2つを鍵としてそれぞれ暗号化する。この暗号化した復号鍵をステップS17で暗号化されたデジタルコンテンツに付加し、それをステップS19で利用者端末1に保存する。

【0045】また、図4を参照するに、購入時の利用者端末1で暗号化されたデジタルコンテンツを復号処理して利用する際には、ステップS21で「端末固有番号」を鍵にしてデジタルコンテンツの復号鍵を復号し、この復号鍵を用いてステップS23で暗号化されたデジタルコンテンツを復号する。

【0046】さらに、図5を参照するに、購入時の利用者端末以外の利用者端末7への複製は、ステップS31で暗号化した復号鍵を添付した暗号化されたデジタルコンテンツを他端末に複製することによって行う。

【0047】複製した端末で初めて暗号化されたデジタルコンテンツを利用する際は、ステップS33で、利用者が「利用者IDと利用者パスワードの組み合わせ」を入力する。これら利用者IDおよび利用者パスワードから、判定部21を用いて判定し（ステップS35）、入力された「利用者IDと利用者パスワードの組み合わせ」が正しかった場合は、ステップS39に進み、暗号化されたデジタルコンテンツの復号鍵を復号し、さらに

ステップS41で、この復号鍵を利用して、暗号化されたデジタルコンテンツを復号する。さらに、複製した端末の「端末固有番号」を鍵にして、再度復号鍵を暗号化し、暗号化されたデジタルコンテンツに添付されている以前の端末の端末固有番号を鍵にして暗号化した復号鍵に上書きする。

【0048】一方、ステップS35で、「利用者IDと利用者パスワードの組み合わせ」が正しくなかった場合は、ステップS37に進み、暗号化されたデジタルコンテンツが正しく復号できなかったことを伝えるエラーメッセージを返し、終了する。

【0049】次に、図6乃至図8を参照して、鍵ファイルと暗号化されたデジタルコンテンツファイルが分離しているタイプにおけるデジタルコンテンツ利用方法を具体的に説明する。

【0050】図6において、ステップS51で、利用者は利用者端末1を操作して、商店端末5からコンピュータネットワーク3を介して、暗号化されたデジタルコンテンツをダウンロードする。また、このダウンロードと同時に、あるいは該暗号化されたデジタルコンテンツの暗号化されていない目次もしくは見出し情報を参照して、当該デジタルコンテンツの購入を決定したときに、ステップS53において暗号化されたデジタルコンテンツの復号鍵を購入する。

【0051】そしてステップS55において、購入した暗号化されたデジタルコンテンツの復号鍵を「利用者IDと利用者パスワードの組み合わせ」と、利用者認証情報取得部11を用いて取り出した「利用者端末の端末識別番号」の2つを鍵として暗号化する。ステップS57で、この暗号化した復号鍵をファイルとし、暗号化されたデジタルコンテンツとともに利用者端末1の記憶部19に保存する。

【0052】また、図7を参照するに、購入時の利用者端末1で暗号化されたデジタルコンテンツを復号処理して利用する際には、ステップS61で「端末固有番号」を鍵にしてデジタルコンテンツの復号鍵を復号し、ステップS63で、この復号鍵を用いて暗号化されたデジタルコンテンツを復号する。

【0053】さらに、図8を参照するに、購入時の利用者端末以外の利用者端末7への複製は、ステップS71で、暗号化されたデジタルコンテンツと2つの暗号化された復号鍵ファイルのすべてを目的の端末に複製することによって行う。

【0054】複製した端末で初めて暗号化されたデジタルコンテンツを利用する際は、ステップS73で、利用者が「利用者IDと利用者パスワードの組み合わせ」を入力する。これら利用者IDおよび利用者パスワードから、判定部21を用いて判定し（ステップS75）、入力された「利用者IDと利用者パスワードの組み合わせ」が正しかった場合は、ステップS79に進み、暗号

化されたデジタルコンテンツの復号鍵を復号し、さらにステップS79で、この復号鍵を利用して、暗号化されたデジタルコンテンツを復号する。さらに、複製した端末の「端末固有番号」を鍵にして、再度復号鍵を暗号化し、以前の端末の端末固有番号を鍵にして暗号化した復号鍵ファイルに上書きする。

【0055】一方、ステップS75で、「利用者IDと利用者パスワードの組み合わせ」が正しくなかった場合は、ステップS77に進み、暗号化されたデジタルコンテンツが正しく復号できなかったことを伝えるエラーメッセージを返し、終了する。

【0056】次に、図9乃至図11を参照して、利用者IDと利用者パスワードの組み合わせで暗号化した復号鍵をICカードに入れるタイプにおけるデジタルコンテンツ利用方法を具体的に説明する。

【0057】なお、ここでは図1(b)に示すように利用者端末1にはカードリーダー31が接続され、利用者がデジタルコンテンツを利用する際にはカードリーダー31を介しての情報の入力が可能であるものとする。

【0058】図9において、ステップS91で、利用者は利用者端末1を操作して、商店端末5からコンピュータネットワーク3を介して、暗号化されたデジタルコンテンツをダウンロードする。また、このダウンロードと同時に、あるいは該暗号化されたデジタルコンテンツの暗号化されていない目次もしくは見出し情報を参照して、当該デジタルコンテンツの購入を決定したときに、ステップS93において暗号化されたデジタルコンテンツの復号鍵を購入する。この購入の際には予めカードリーダー31を利用者端末1に接続し、利用者の「利用者ID」等が記録されたICカードを挿入しておく。

【0059】そしてステップS95において、購入した暗号化されたデジタルコンテンツの復号鍵を「利用者IDと利用者パスワードの組み合わせ」と、利用者認証情報取得部11を用いて取り出した「利用者端末の端末固有番号」の2つを鍵として暗号化する。

【0060】さらに、ステップS97で、この暗号化した2つの復号鍵のうち「利用者端末の端末固有番号」で暗号化した復号鍵を暗号化されたデジタルコンテンツとともに利用者端末1の記憶部19に保存する。そして「利用者IDと利用者パスワードの組み合わせ」で暗号化した復号鍵は、ステップS99で、カードリーダーに挿入されているICカードに保存される。

【0061】また、図10を参照するに、購入時の利用者端末1で暗号化されたデジタルコンテンツを利用する際には、ステップS101で「端末固有番号」を鍵にしてデジタルコンテンツの復号鍵を復号し、ステップS103で、この復号鍵を用いて暗号化されたデジタルコンテンツを復号する。

【0062】さらに、図11を参照するに、購入時の利用者端末以外の利用者端末7への複製は、ステップS1

11で、暗号化されたデジタルコンテンツのみを複製することによって行う。

【0063】複製した端末で初めて暗号化されたデジタルコンテンツを利用する際は、ステップS113で、複製した端末にカードリーダー31を接続して利用者のICカードを挿入し、利用者が「利用者IDと利用者パスワードの組み合わせ」を入力する。ステップS115において、判定部21を用いて判定し、入力された「利用者IDと利用者パスワードの組み合わせ」が正しかった場合は、ステップS119に進み、ICカードに保存されている暗号化されたデジタルコンテンツの復号鍵を復号し、この復号鍵を利用して、暗号化されたデジタルコンテンツを復号する。さらに、ステップS121で、複製した端末の「端末固有番号」を鍵にして、再度復号鍵を暗号化した復号鍵ファイルを生成する。

【0064】一方、ステップS115で、「利用者IDと利用者パスワードの組み合わせ」が正しくなかった場合は、ステップS117に進み、暗号化されたデジタルコンテンツが正しく復号できなかったことを伝えるエラーメッセージを返し、終了する。

【0065】上述してきたように、本実施形態においては、暗号化されたデジタルコンテンツの復号鍵を、端末識別装置を用いて取り出した「端末固有番号」と「利用者IDと利用者パスワードの組み合わせ」のそれぞれを鍵として暗号化する。

【0066】また、暗号化されたデジタルコンテンツを利用する場合は、「端末識別情報」か「利用者IDと利用者パスワードの組み合わせ」のどちらかを鍵として暗号化されたデジタルコンテンツの復号鍵を復号し、デジタルコンテンツの復号を可能にする。

【0067】また、正規の利用者でも他端末へ複製できないという問題は、暗号化されたデジタルコンテンツの複製を可能とし、正規の利用者が複製後初めて復号するときに「利用者IDと利用者パスワードの組み合わせ」を入力して正規の利用者であると認証された場合のみ復号することによって解決する。これにより、正規の利用者以外他端末への複製を防止することができる。

【0068】この際、入力された「利用者IDと利用者パスワードの組み合わせ」が正しいかどうかを「利用者IDおよび利用者パスワード判定装置」を用いて判定を行う。正しくない場合は、正しく復号鍵を復号できない旨を伝えるエラー処理を行う。入力された「利用者IDと利用者パスワードの組み合わせ」が正しい場合には、正しく復号鍵が復号され、暗号化されたデジタルコンテンツを復号する。暗号化されたデジタルコンテンツが復号できた場合は、新たに格納された端末の端末識別番号で暗号化されたデジタルコンテンツの復号鍵を再度暗号化して、以前の端末識別番号で暗号化されたデジタルコンテンツの復号鍵に上書きしておく。

【0069】また、利用者が一度でも「利用者IDと利

10

20

30

40

50

用者パスワードの組み合わせ」で認証したデジタルコンテンツに対してはそれ以後「端末固有番号」を利用して復号することによって、デジタルコンテンツを利用する度に「利用者IDと利用者パスワードの組み合わせ」を入力しなければならないという問題を解決する。

【0070】前述の手段により、他端末への複製に対しては、複製した暗号化されたデジタルコンテンツに対し、正規の利用者が「利用者IDと利用者パスワードの組み合わせ」を入力することによって復号鍵を復号することによって可能とし、同時に正規の利用者以外による他端末への複製を防止する。また、暗号化されたデジタルコンテンツの復号鍵を一度でも「利用者IDと利用者パスワードの組み合わせ」で復号した端末では、それ以後「端末固有番号」を利用して復号鍵の復号をするため「利用者IDと利用者パスワードの組み合わせ」を入力する必要がなくなる。

【0071】なお、このようなコンテンツ利用はコンテンツ利用プログラムにより実現され、該プログラムは記録媒体に記録して提供される。

【0072】上述してきたように、本実施形態によれば、暗号化されたデジタルコンテンツの復号鍵を、「利用者IDと利用者パスワードの組み合わせ」と端末識別装置を用いて取り出した「端末固有番号」の2つを鍵として暗号化し、この2つの暗号化された復号鍵を使い分けるようにしたので、暗号化されたデジタルコンテンツ利用方法は以下の効果を持つ。

【0073】1. 「利用者IDと利用者パスワードの組み合わせ」か「端末固有番号」のどちらか片方を鍵として、暗号化されたデジタルコンテンツの復号鍵を復号し、暗号化されたデジタルコンテンツの復号を可能にする。

【0074】2. 他端末へ暗号化されたデジタルコンテンツの複製を行った場合は、複製したデジタルコンテンツの初回復号時に利用者が「利用者IDと利用者パスワードの組み合わせ」を入力することによってのみ可能とする。これにより正当な利用者の複製を可能とすると同時に不正使用を防止する。

【0075】3. 暗号化されたデジタルコンテンツの復号鍵を1度でも「利用者IDと利用者パスワードの組み合わせ」で復号した端末では、それ以後「端末固有番号」で暗号化されたデジタルコンテンツの復号鍵で復号を行い、利用者が「利用者IDと利用者パスワードの組み合わせ」を入力する手間を省くことを可能とする。

【0076】

【発明の効果】以上説明したように、本発明は、暗号化されたコンテンツの復号鍵を、利用者認証情報と、利用端末の端末識別情報との2つを鍵としてそれぞれ暗号化し、この暗号化により得られた2つの復号鍵を使い分けるようにしたので、暗号化されたデジタルコンテンツの復号鍵を1度でも利用者認証情報で復号した端末では、

それ以後、利用端末の端末識別情報で暗号化されたデジタルコンテンツの復号鍵で復号を行い、利用者が利用者認証情報を入力する手間を省くことを可能とする。

【図面の簡単な説明】

【図1】本発明に係るデジタルコンテンツ利用システムの概略の構成を示すブロック図である。

【図2】本発明の概要を明確にするためのブロック図である。

【図3】鍵ファイルをカプセルに付加するタイプにおける暗号化されたデジタルコンテンツの不正使用の防止処理手順を示すフローチャートである。

【図4】購入端末での復号処理手順を示すフローチャートである。

【図5】複製した端末での復号処理手順を示すフローチャートである。

【図6】鍵ファイルを分離するタイプにおける暗号化されたデジタルコンテンツの不正使用の防止処理手順を示すフローチャートである。

【図7】購入端末での復号処理手順を示すフローチャートである。

【図8】複製した端末での復号処理手順を示すフローチャートである。

【図9】利用者IDと利用者パスワードの組み合わせで暗号化した復号鍵をICカードに入れるタイプにおける暗号化されたデジタルコンテンツの不正使用の防止処理手順を示すフローチャートである。

【図10】購入端末での復号処理手順を示すフローチャートである。

【図11】複製した端末での復号処理手順を示すフローチャートである。

【符号の説明】

- 1 利用者端末（正規利用者）
- 3 コンピュータネットワーク
- 5 商店端末
- 7 利用者端末（正規利用者以外）
- 11 利用者認証情報取得部
- 13 コンテンツ取得部
- 13a 暗号化コンテンツ取得部
- 13b 復号鍵取得部
- 15 端末識別番号取得部
- 17 暗号化部
- 17a 復号鍵暗号化部
- 17b 所定値暗号化部
- 19 記憶部
- 21 判定部
- 23 復号化部
- 23a 暗号化復号鍵復号化部
- 23b コンテンツ復号化部
- 25 コンテンツ利用部
- 31 カードリーダー



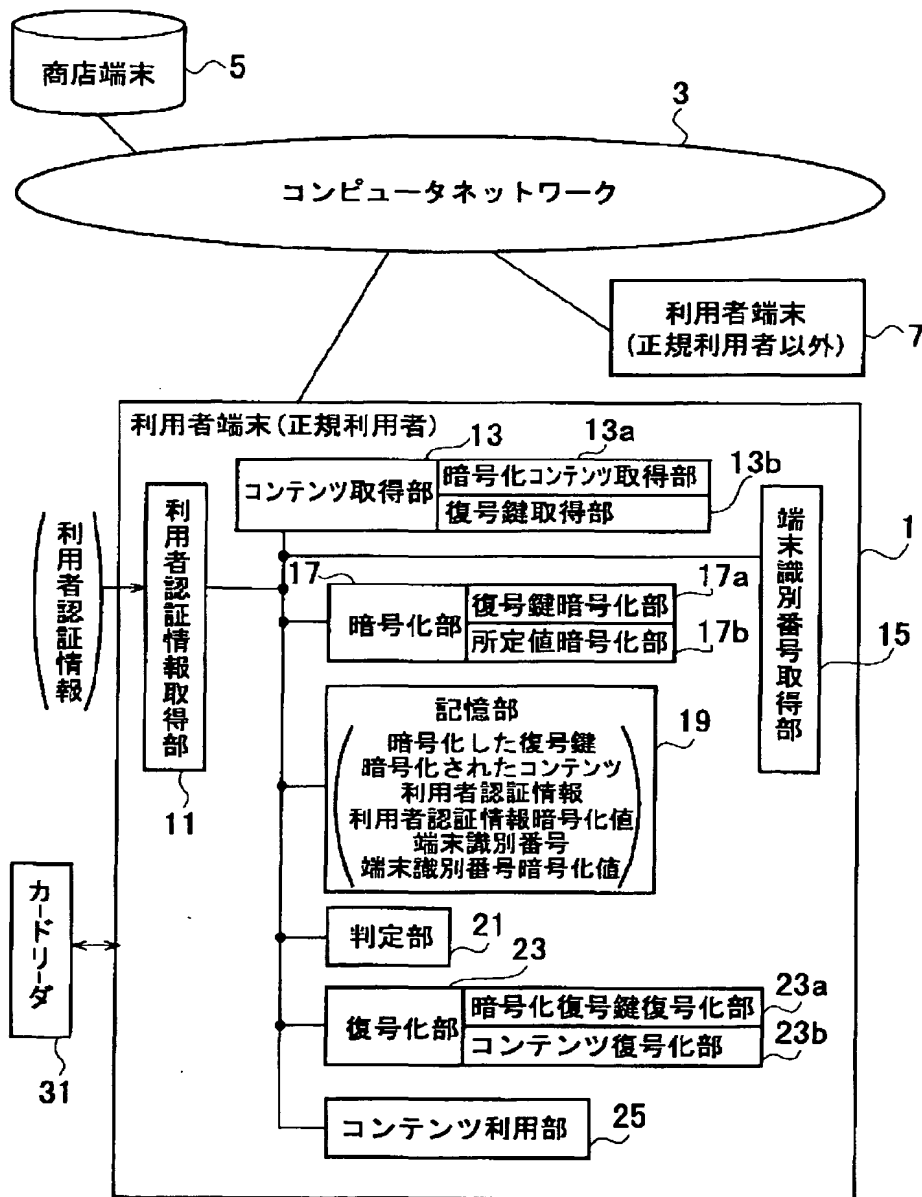
## 【要約】

【課題】 本発明は、利用者が利用者認証情報を入力する手間を省くことを可能とし、正規の利用者による使用を制限することなくコンテンツの不正使用を防止することのできるコンテンツ利用方法およびその装置とコンテンツ利用プログラムを記録した記録媒体を提供することを目的とする。

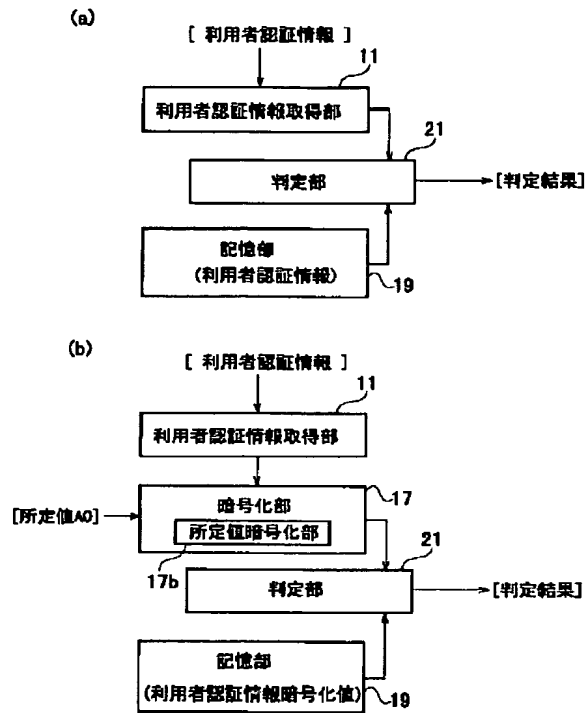
【解決手段】 暗号化されたコンテンツを復号する第1の復号鍵とを取得し、所定の端末識別情報及び提供される利用者認証情報で復号鍵をそれぞれ暗号化して得られ

る第2、第3の復号鍵を記憶する記憶手段と、暗号化されたコンテンツを復号するに際し、この暗号化されたコンテンツを復号する利用端末の端末識別情報により前記記憶手段に記憶される第2の復号鍵の復号が可能かどうかを判定する判定手段で復号可能であると判定されたときには、この端末識別情報により前記暗号化された第2の復号鍵を復号化して第1の復号鍵を得、不可能であると判定されたときには、前記利用者認証情報により前記暗号化された第3の復号鍵を復号化して第1の復号鍵を得る復号手段とを備えて構成される。

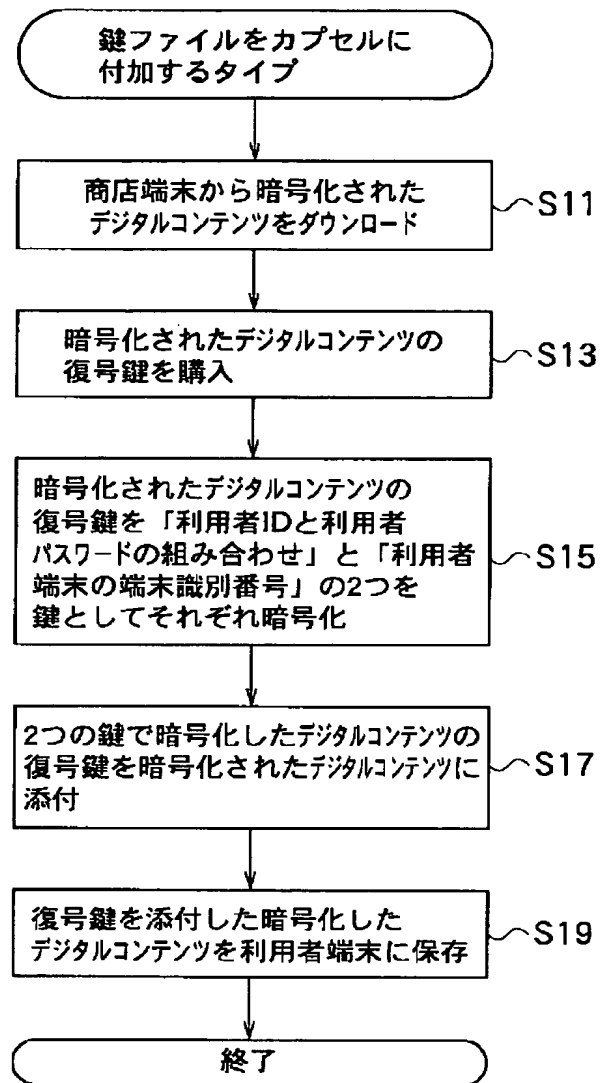
【図1】



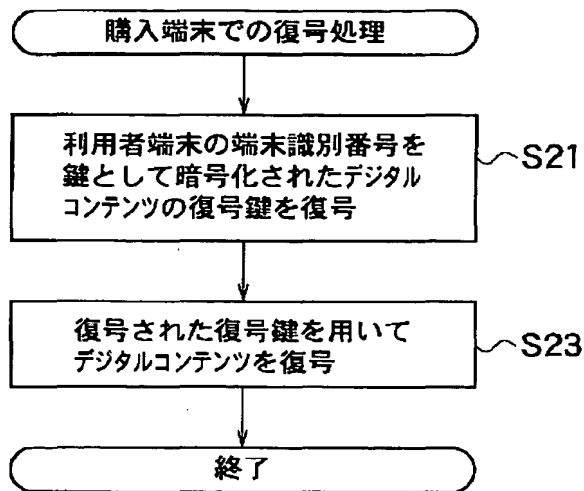
【図2】



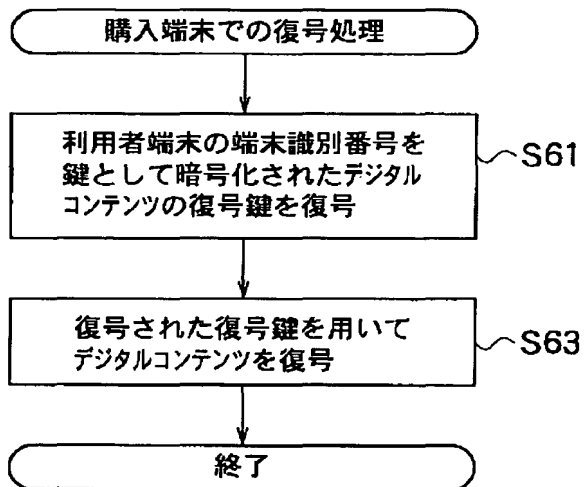
【図3】



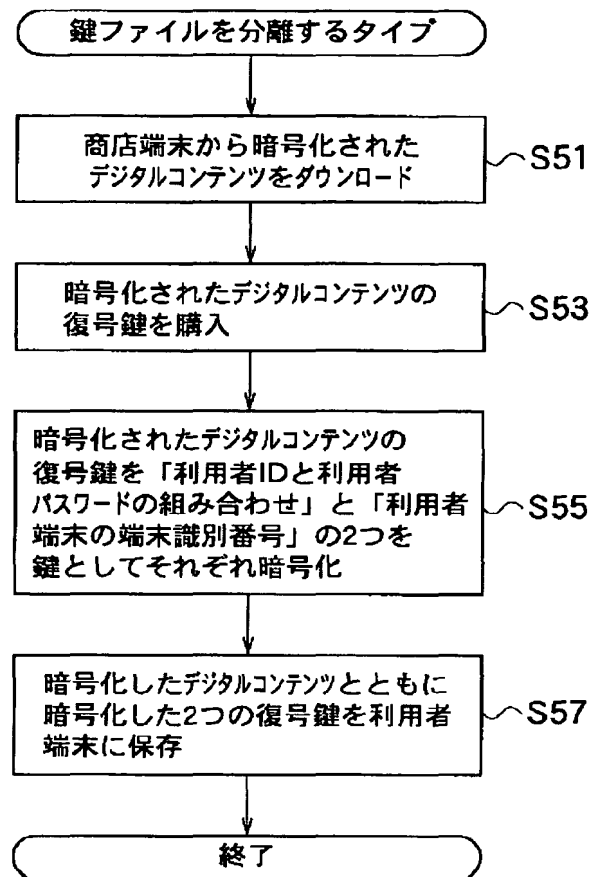
【図4】



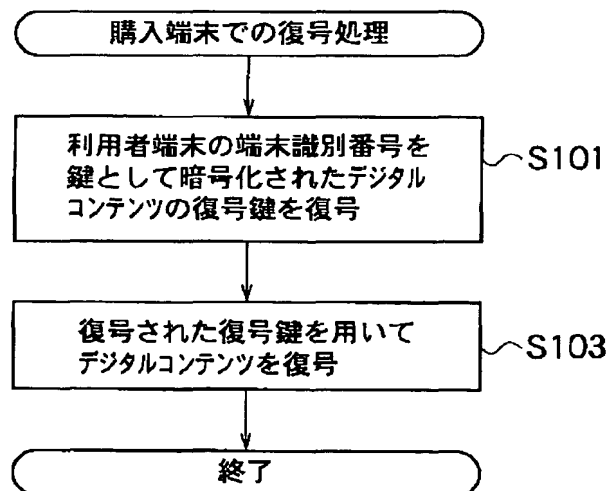
【図7】



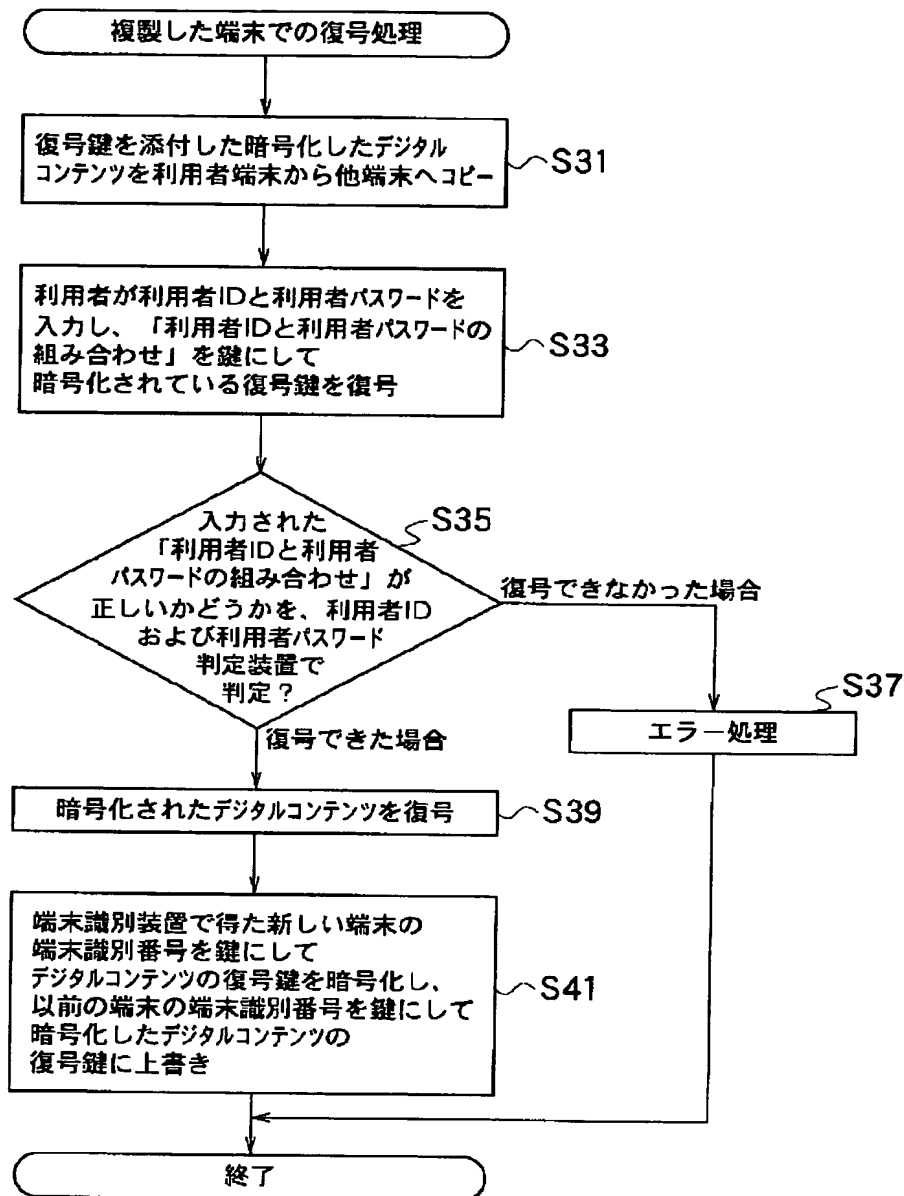
【図6】



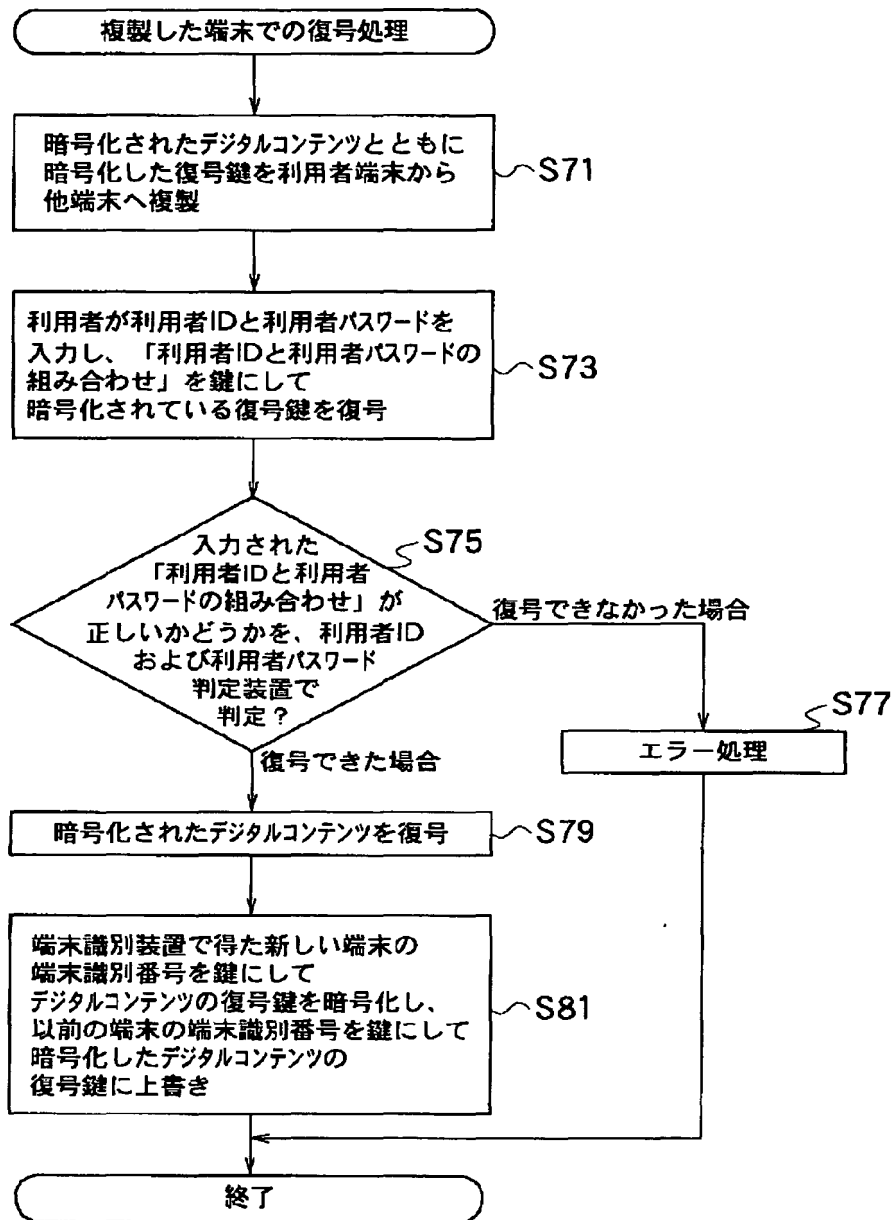
【図10】



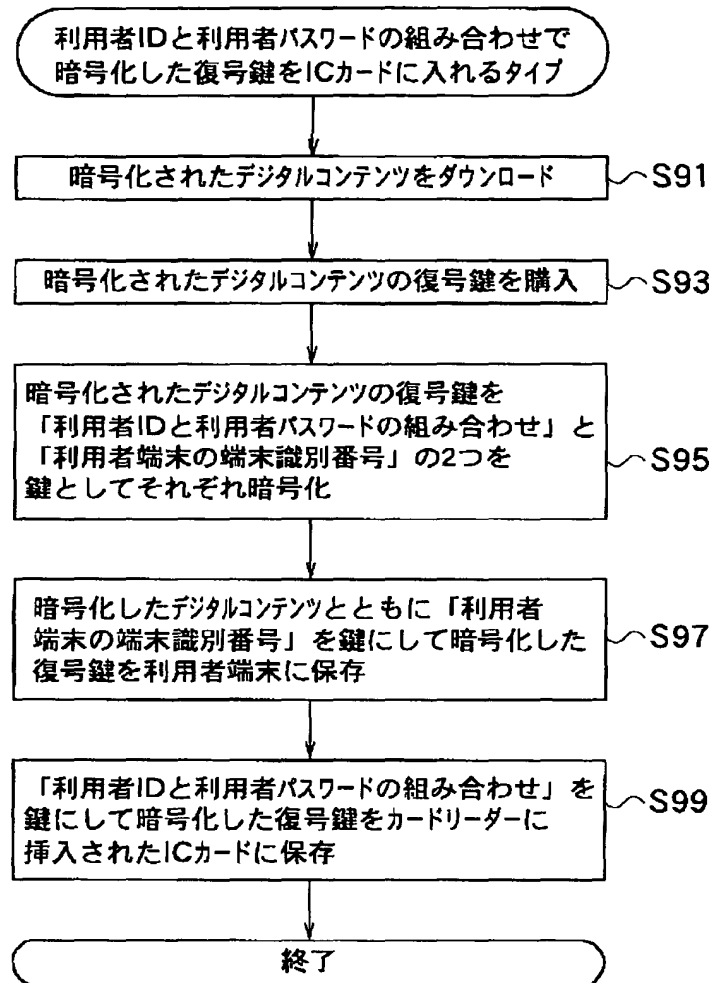
【図5】



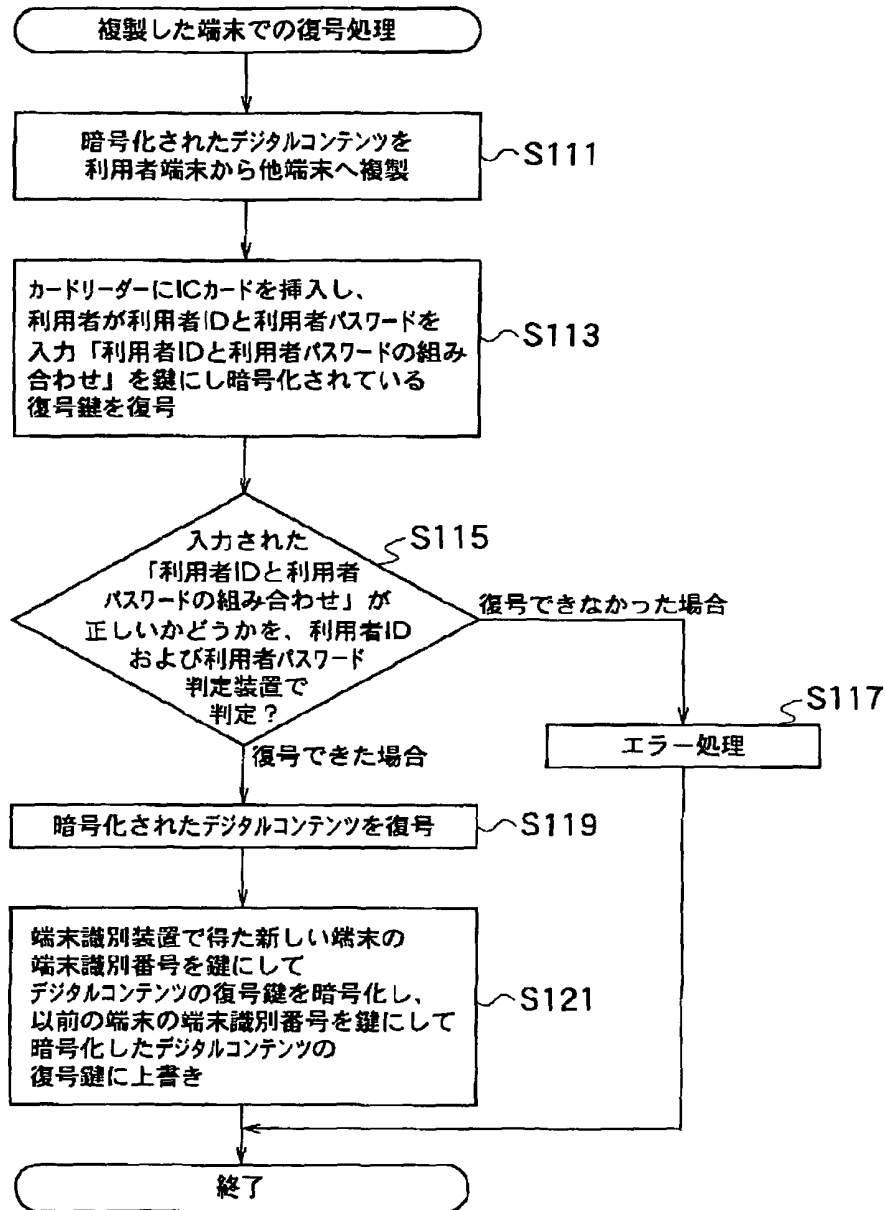
【図8】



【図9】



【図11】



フロントページの続き

(72)発明者 曾根岡 昭直  
東京都新宿区西新宿三丁目19番2号 日  
本電信電話株式会社内

(56) 参考文献 明石 他, “インターネットを用いた  
情報流通プラットフォーム: INFOKE  
ET-I”, NTT R&D, Vol.  
46, No. 2 (平9. 2. 10) p. 107  
-114

庵 他, “情報販売における不正コピー  
防止方式の提案”, 情報処理学会第57  
回(平成10年後期)全国大会講演論文集  
(3) (平10. 10. 5) p. 3・23-  
3・24

庵 他, “不正コピー防止を考慮した  
情報販売方式”, 情報処理学会研究報  
告, Vol. 99, No. 4 (DSP-  
91) p. 139-144

(58) 調査した分野(Int.Cl.<sup>7</sup>, DB名)

H04L 9/00

G09C 1/00